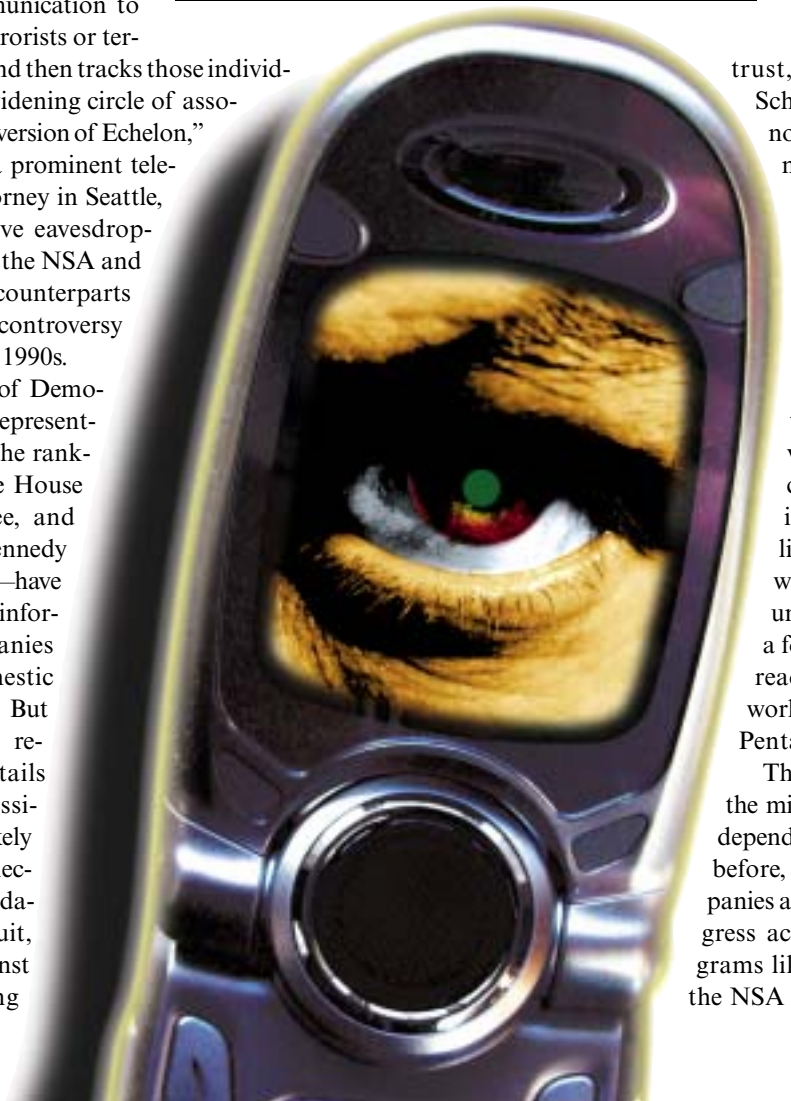
ARTICLES

HOW BIG TELECOM MAY BE HELPING GOVERNMENT SPIES

WATCHING WHAT YOU SAY

by TIM SHORROCK

Two months after the *New York Times* revealed that the Bush Administration ordered the National Security Agency to conduct warrantless surveillance of American citizens, only three corporations—AT&T, Sprint and MCI—have been identified by the media as cooperating. If the reports in the *Times* and other newspapers are true, these companies have allowed the NSA to intercept thousands of telephone calls, fax messages and e-mails without warrants from a special oversight court established by Congress under the 1978 Foreign Intelligence Surveillance Act (FISA). Some companies, according to the same reports, have given the NSA a direct hookup to their huge databases of communications records. The NSA, using the same supercomputers that analyze foreign communications, sifts through this data for key words and phrases that could indicate communication to or from suspected terrorists or terrorist sympathizers and then tracks those individuals and their ever-widening circle of associates. "This is the US version of Echelon," says Albert Gidari, a prominent telecommunications attorney in Seattle, referring to a massive eavesdropping program run by the NSA and its English-speaking counterparts that created a huge controversy in Europe in the late 1990s.



So far, a handful of Democratic lawmakers—Representative John Conyers, the ranking Democrat on the House Judiciary Committee, and Senators Edward Kennedy and Russell Feingold—have attempted to obtain information from companies involved in the domestic surveillance program. But they've largely been rebuffed. Further details about the highly classified program are likely to emerge as the Electronic Frontier Foundation pursues a lawsuit, filed January 31, against AT&T for violating privacy laws by giving the NSA direct access to its telephone records database and Internet transaction logs. On February 16 a federal judge gave the Bush Administration until March 8 to turn over a list of internal documents related to two other lawsuits, filed by the American Civil Liberties Union and the Electronic Privacy Information Center, seeking an injunction to end the program.

Despite the President's rigorous defense of the program, no company has dared to admit its cooperation publicly. Their reticence is understandable: The Justice Department has launched a criminal investigation of the government officials who leaked the NSA story to the *Times*, and many constitutional scholars and a few lawmakers believe the program is both illegal and unconstitutional. And the companies may be embarrassed at being caught—particularly AT&T, which spent millions advertising its global services during the Winter Olympics. "It's a huge betrayal of the public trust, and they know it," says Bruce Schneier, the founder and chief technology officer of Counterpane Internet Security, a California consulting firm.

Corporations have been cooperating with the NSA for half a century. What's different now is that they appear to be helping the NSA deploy its awesome computing and data-mining powers inside the United States in direct contravention of US law, which specifically bans the agency from collecting information from US citizens living inside the United States. "They wouldn't touch US persons before unless they had a FISA warrant," says a former national security official who read NSA intercepts as part of his work for the State Department and the Pentagon.

This is happening at a time when both the military and its spy agencies are more dependent on the private sector than ever before, and an increasing number of companies are involved. In the 1970s, when Congress acted to stop domestic spying programs like Operation Shamrock, in which the NSA monitored overseas telegrams and

phone calls, the communications industry was in its infancy. "It was basically Western Union for cables, and AT&T for the telephone," says James Bamford, who revealed the existence of the NSA in his famous book *The Puzzle Palace* and is a plaintiff in the ACLU lawsuit. "It's much more complicated now." In fact, today's global telecom market includes dozens of companies that compete with AT&T, Sprint and MCI for telephone and mobile services, as well as scores of Internet service providers like Google, Yahoo! and AOL that offer e-mail, Internet and voice connections to customers around the world. They are served by multinational conglomerates like Apollo, Flag Atlantic and Global Crossing, which own and operate the global system of undersea fiber-optic cables that link the United States to the rest of the world. Any one of them could be among the companies contacted by intelligence officials when President Bush issued his 2002 executive order to obtain surveillance without FISA approval.

'The telcos have been participating in surveillance activities for decades…it's nothing new to them.' —Kenneth Bass, former Justice official

Nobody's talking, though. Asked if AT&T, which was recently acquired by SBC Communications, is cooperating with the NSA, AT&T spokesman Walt Sharp said, "We don't comment on national security matters." He referred me to a recent AT&T letter to Representative Conyers, which stated that AT&T "abides by all applicable laws, regulations and statutes in its operations and, in particular, with respect to requests for assistance from governmental authorities." MCI, which was acquired in January by Verizon, and Sprint, which recently merged with Nextel Communications, declined to comment. Attorney Gidari, who has represented Google, T-Mobile, Nextel and Cingular Wireless (now part of AT&T), does admit that "some companies, both telecom and Internet," were asked to participate in the NSA program. But he claims that only a limited number agreed. "The list of those who said no is much longer than most people think," he says.

The NSA, some analysts say, may have sought the assistance of US telecoms because most of the world's cable operators are controlled by foreign corporations. Apollo, for example, is owned by Britain's Cable & Wireless, while Flag Atlantic is owned by the Reliance Group of India. Much of the international "transit traffic" carried by the cable companies flows through the United States (this is particularly true of communications emanating from South America and moving between Asia and Europe). The NSA could get access to this traffic by sending a submarine team to splice the cables in international waters, as the agency once did to the Soviet Union's undersea military cables. But that is an extremely expensive proposition, and politically dicey to boot—which is where the US telecoms come in. "Cooperation with the telcos doesn't make NSA surveillance possible, but it does make it cheaper," says Schneier, the technology consultant.

According to Alan Mauldin, a senior research analyst with TeleGeography Research in Washington, DC, it would be possible for US intelligence operatives to gain access to transit traffic from anywhere in the country with the cooperation of a US company. "You could be inland, at an important city like New York or Washington, DC, where networks interconnect, and you could have the ability to tap into the whole network for not only that city but between that city and the rest of the world," he says. Foreign-owned cable operators, says Gidari, are also required by US law to maintain security offices manned by US citizens, with background checks and security clearances at the landing sites in Oregon, Florida, New Jersey and other states where fiber-optic cables come ashore.

The government has gone to great lengths to insure law-enforcement access to foreign-owned telecom companies. Take the example of Global Crossing, which owns several undersea cable systems and claims to serve more than 700 carriers, mobile operators and ISPs. Three years ago, as Global Crossing was emerging from one of the largest bankruptcies in US history, it was purchased by ST Telemedia, which is partly owned by the government of Singapore. As part of the US approval process (which occurred at a time when Global Crossing was being advised by Richard Perle, then-chairman of Donald Rumsfeld's Defense Policy Board), the company signed an unprecedented Network Security Agreement with the FBI and the Defense Department. Under the agreement, which is on file with the Federal Communications Commission, Global Crossing pledged that "all domestic communications" would pass through a facility "physically located in the United States, from which Electronic Surveillance can be conducted pursuant to lawful US process." (Global Crossing declined to comment.) Legal experts say the wording is significant in the context of the NSA spying flap, but cautioned not to read too much into it. "These agreements are not uncommon in the industry," says James Andrew Lewis, director of the Technology and Public Policy Program at the Center for Strategic and International Studies in Washington. "They provide assurances that US interests won't suffer damage with foreign ownership."

History proves a good guide to how the NSA would go about winning cooperation from a telecom company. When telephone and telegraph companies began assisting the NSA during the 1940s, only one or two executives were in on the secret. That kind of arrangement continued into the 1970s, and is probably how cooperation with the NSA works today, says Kenneth Bass III, a Justice Department official during the Carter Administration. "Once the CEO approved, all the contacts [with the intelligence agencies] would be worked at a lower level," he says. "The telcos have been participating in surveillance activities for decades—pre-FISA, post-FISA—so it's nothing new to them." Bass, who helped craft the FISA law and worked with the NSA to implement it, adds that he "would not be surprised at all" if cooperating executives received from the Bush Administration "the same sort of briefing, but much more detailed and specific than the FISA court got when [the surveillance] was first approved."

Tim Shorrock (timshorrock@gmail.com), a longtime contributor to The Nation*, is writing a book for Simon & Schuster about corporate influence on US foreign policy.* *Research assistance was provided by the Investigative Fund of The Nation Institute.*

For US intelligence officials looking for allies in the industry, AT&T, MCI and Sprint have a lot to offer. In 2002, when the spying program began, AT&T's CEO was C. Michael Armstrong, the former CEO of Hughes Electronic Corp. At the time, Armstrong was also chairman of the Business Roundtable's Security Task Force, where he was instrumental in creating CEO COM LINK, a secure telecommunications system that allows the chief executives of major US corporations to speak directly to senior members of Bush's Cabinet during national emergencies. Randall Stephenson, a former SBC Communications executive who is now AT&T's chief operating officer, is a member of the National Security Telecommunications Advisory Committee, a group of executives from the communications and defense industries who advise the President on security issues related to telecom.

Those executives, all of whom hold security clearances, meet at the White House once a year—Vice President Cheney was the speaker at their last meeting—and hold quarterly conference calls with high-ranking officials. (Asked if the NSA surveillance was ever discussed at these sessions, committee spokesman Stephen Barrett said, "We do not participate in intelligence gathering.") AT&T also makes no bones about its national security work. When SBC was preparing to acquire the company last year, the two companies underscored their ties with US intelligence in joint comments to the FCC. "AT&T's support of the intelligence and defense communities includes the performance of various classified contracts," the companies said, pointing out that AT&T "maintains special secure facilities for the performance of classified work and the safeguarding of classified information."

'Arguing that this is legal is basically saying we're in a police state.'
—Bruce Schneier, technology consultant

MCI, too, is a major government contractor and was highly valued by Verizon in part because of its work in defense and intelligence. Nicholas Katzenbach, the former US Attorney General who was appointed chairman of MCI's board after the spectacular collapse of its previous owner, WorldCom, reiterated MCI's intelligence connections in a 2003 statement to the Senate Judiciary Committee. "We are especially proud," he wrote, "of our role in supporting our national-security agencies' infrastructure, and we are gratified by the many positive comments about our service from officials at the US Department of Defense and other national-security agencies." MCI's general counsel—who would presumably have a say in any decision to cooperate with the NSA—is William Barr. He is a former assistant general counsel at the Central Intelligence Agency and served as Attorney General during the Administration of President George H.W. Bush.

Sprint Nextel is top-loaded with executives with long experience in national security and defense. Chairman and CEO Gary Forsee is a member of Bush's telecom council (as is Lawrence Babbio, the vice chairman and president of Verizon). Keith Bane, a company director, recently retired from a twenty-nine-year career with Motorola, which has worked closely with US intelligence for decades. William Conway Jr. and former FCC chairman William Kennard are managing directors of the Carlyle Group, the Washington private equity fund that invests heavily in the military and has extensive contacts in the Bush Administration.

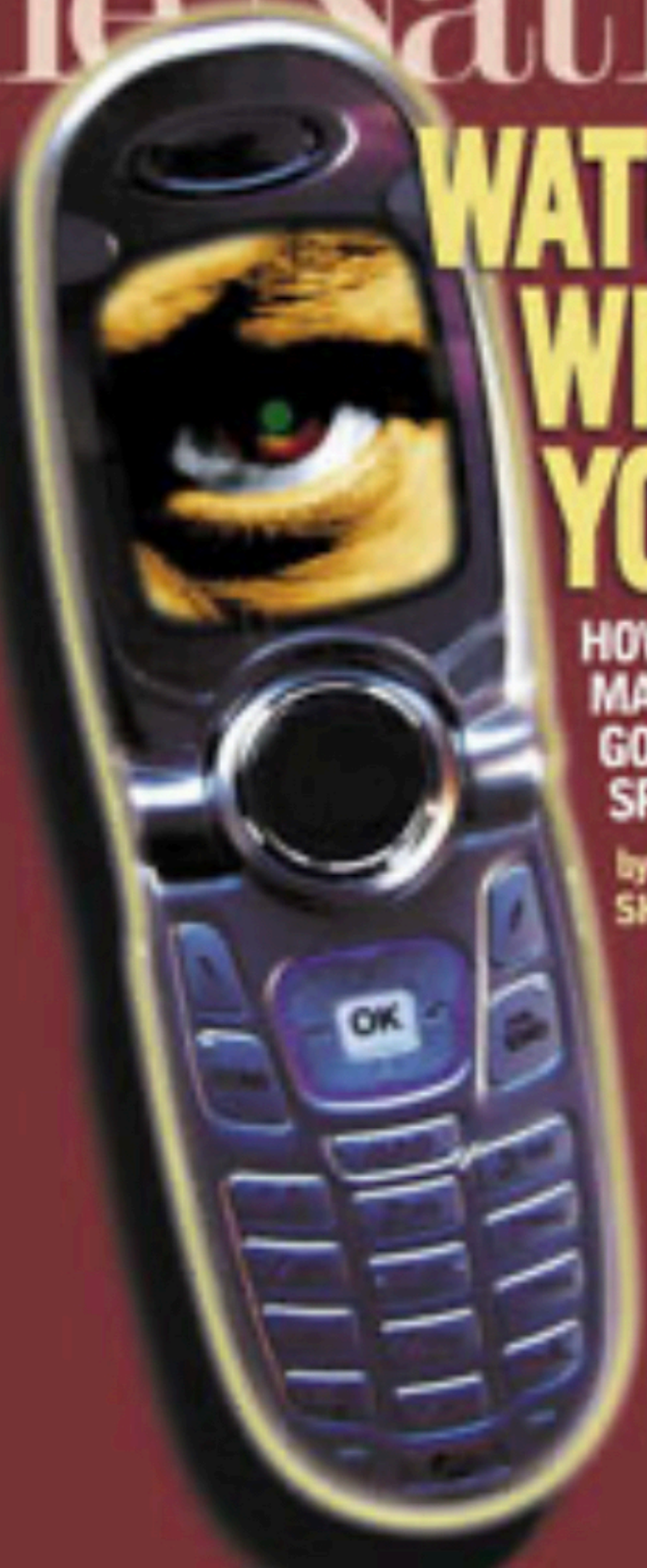
There's another group of companies, largely overlooked, that could also be cooperating with the NSA. These are firms clustered around the Beltway that contract with the agency to provide intelligence analysts, data-mining technologies and equipment used in the NSA's global signals-intelligence operations. The largest of them employ so many former intelligence officials that it's almost impossible to see where the government ends and the private sector begins. Booz Allen Hamilton, the prime contractor for Trailblazer, a huge NSA project updating its surveillance and eavesdropping infrastructure, employs several NSA alumni, including Mike McConnell, its vice president, who retired as NSA director in 1996. (Ralph Shrader, the company's CEO, joined Booz Allen in 1978 after serving in senior positions with Western Union and RCA, both of which cooperated with the NSA on Operation Shamrock.) SI International, a software and systems engineering company with NSA contracts, recently hired Harry Gatanas, the NSA's former director of acquisitions and outsourcing, to oversee its $250-million-a-year business with US intelligence and the Pentagon. Science Applications International Corporation, another big NSA contractor, is run by executives with long histories in military intelligence, including COO Duane Andrews, a former Assistant Secretary of Defense for Command, Control, Communications and Intelligence.

Are firms that cooperate with the NSA legally culpable? Bamford, who is not a lawyer but probably knows more about the NSA than any American outside government, says yes. "The FISA law is very clear," he says. "If you don't have a warrant, you're in violation, and the penalty is five years and you can be sued by the aggrieved parties." Kevin Bankston, an attorney for the Electronic Frontier Foundation, adds that US law "not only prohibits unauthorized wiretapping; it also prohibits unauthorized disclosure or use of illegally wiretapped information. As long as you were doing that, you're potentially liable." Schneier, the technology consultant, harbors no doubts either. "Arguing that this is legal is basically saying we're in a police state."

But Gidari, the Seattle telecom attorney, believes that companies would be insulated from legal challenges if they had assurances from the government that the program was within the law. He also says Congress has passed legislation granting immunity to companies operating under "statutory grants of authority" from the government. "It's not a slamdunk, but it is a good-faith defense," he says. Former Justice Department official Bass agrees but says reliance on oral requests from US officials is another matter: "If they didn't get the type of legal assurances the FISA provides for"—such as a written statement from the Attorney General—"there could be some legal exposure." But a full airing of the legal issues raised by the surveillance program may be a long time coming. "The likelihood of any enforcement absent a change in administration is zero," Bass says. ■

The Nation.

MAR. 20, 2006
www.thenation.com



WATCHING WHAT YOU SAY

HOW BIG TELECOM MAY BE HELPING GOVERNMENT SPIES

by TIM SHORROCK